

UNITED STATES DISTRICT COURT

for the
Eastern District of Virginia

In the Matter of the Search of)
 (Briefly describe the property to be searched)
 or identify the person by name and address) Case No. 1:17-SW-19
 INFORMATION STORED IN THE SERVER THAT IS)
 ASSOCIATED WITH IP ADDRESS 104.232.35[.]104 AND IS)
 LOCATED AT PREMISES CONTROLLED BY NET3 INC)

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Western District of New York
 (identify the person or describe the property to be searched and give its location):
 See Attachment A

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized):
 See Attachment B

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property.

YOU ARE COMMANDED to execute this warrant on or before February 2, 2017

(not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge the Honorable Theresa C. Buchanan
 (name)

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box) ☐ for _____ days (not to exceed 30)
☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 1/19/17 3:50

Theresa Carroll Buchanan
 United States Magistrate Judge
 Judge's signature

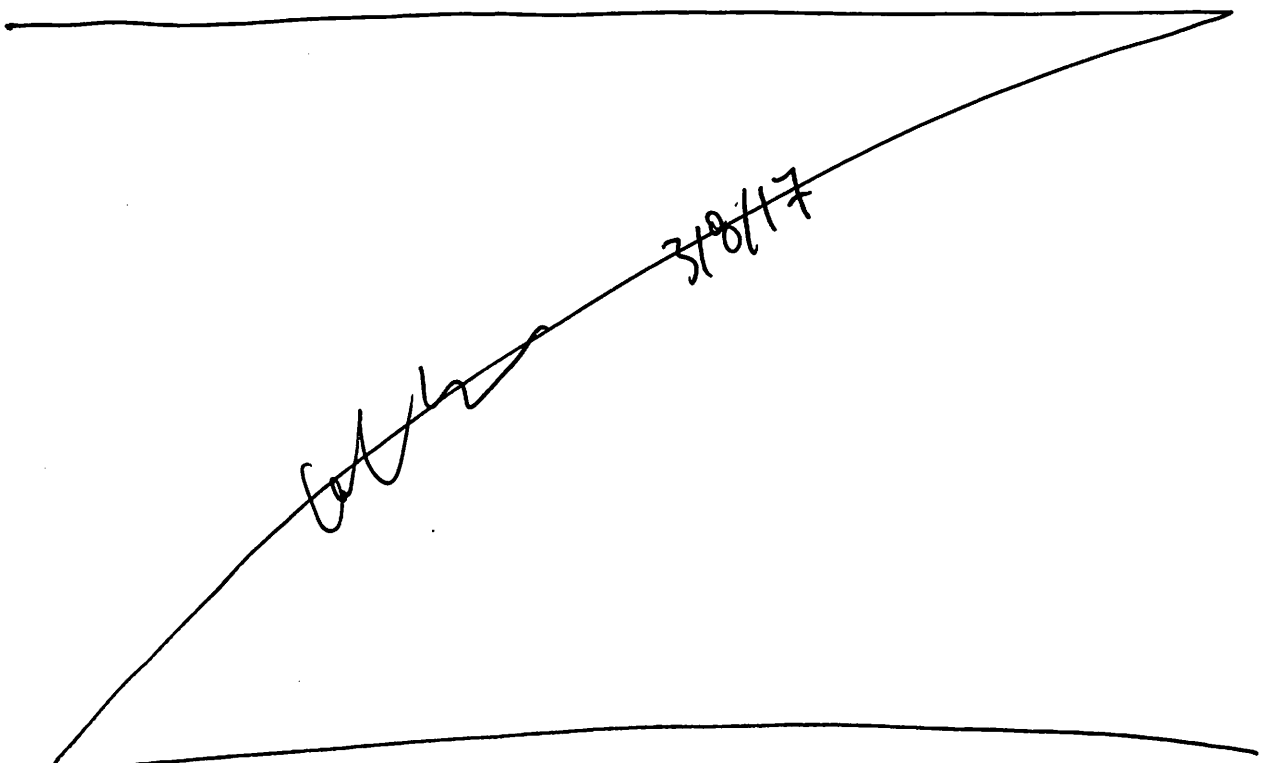
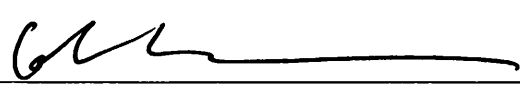
City and state: Alexandria, Virginia

The Honorable Theresa C. Buchanan, U.S. Magistrate Judge
 Printed name and title



10/1/47

10/1/47

Return		
Case No.: 1:17-SW-19	Date and time warrant executed: 1/19/17 @ 1732 EST	Copy of warrant and inventory left with: Net3 Inc.
Inventory made in the presence of: SA TIMOTHY CHAFFEY, USPS OIG		
Inventory of the property taken and name of any person(s) seized: Information pertaining to the captioned server and associated customer. 		
Certification		
I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.		
Date: 3/8/17	 Executing officer's signature Cole Ashcraft, Special Agent, USPS OIG Printed name and title	

ATTACHMENT A

Information stored on the TARGET SERVER.

The TARGET SERVER is a server associated with the Internet Protocol address 104.232.35[.]104. The TARGET SERVER is located at premises owned, maintained, controlled, or operated by Net3 Inc., a U.S. provider of electronic communication and remote computing services accepting correspondence at 170 - 422 Richards St, Vancouver, BC V6B 2Z4, Canada.

ATTACHMENT B

PARTICULAR THINGS TO BE SEIZED

I. Information to be disclosed by Net3 Inc. (Net3)

To the extent that the information described in Attachment A is within the possession, custody, or control of Net3, Net3 is required to disclose the following information to the government:

- a. an image copy of all data and information electronically stored in the TARGET SERVER, to include the contents of memory if technically feasible, and any data previously preserved, pursuant to 18 U.S.C. § 2703(f);
- b. all backups of the TARGET SERVER taken between January 1, 2015 and the present;
- c. all information in the possession of Net3 that might identify the person or persons who operate, pay for, or are associated with the TARGET SERVER, including names, addresses, telephone numbers and other identifiers, e-mail addresses, business information, the length of service (including start date), types of services utilized, means and source of payment for services (including any credit card or bank account number), and information about any domain name registration;
- d. all records pertaining to communications between Net3 and any person regarding the account or identifier, including contacts with support services and records of actions taken.
- e. records and content of network traffic between the TARGET SERVER and any party between January 1, 2015 and the present, including network flow data and full packet captures

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. §§ 1029, 1030, 1343, 2511, or 2512, occurring on or after January 1, 2009, including all data on the server and information pertaining to the following matters:

- a. Unauthorized access to protected computer systems
- b. Unlawful interception of electronic communications, including the development, acquisition, possession, or use of any electronic, mechanical, or other device to intercept electronic communications;
- c. Wire and access device fraud;
- d. Preparatory steps taken in furtherance of this scheme, including the acquisition, development, and operation of technical infrastructure or software needed to support the scheme;
- e. Evidence indicating the server owner or operator's state of mind as it relates to the crime under investigation;
- f. Records of who used, owned, or controlled the TARGET SERVER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

- g. Records of software that would allow others to control the TARGET SERVER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- h. Records of the lack of such malicious software;
- i. Records of counter-forensic programs (and associated data) that are designed to eliminate data from the TARGET SERVER;
- j. Records of the times the TARGET SERVER was used;
- k. Records that might identify the persons leasing or operating the TARGET SERVER and their current whereabouts, including names, addresses, telephone numbers and other identifiers, e-mail addresses, business information, the length of service (including start date), means and source of payment for services (including any credit card or bank account number), and information about any domain name registration;
- l. Records identifying the types of service utilized by the user;
- m. Records pertaining to communications between Net3 and any person regarding the TARGET SERVER, including contacts with support services and records of actions taken;
- n. Contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored,

including hard drives, random-access memory, and any other form of computer or electronic storage.